ISSN 1561-2430 (Print)
ISSN 2524-2415 (Online)
УДК 511.622
https://doi.org/10.29235/1561-2430-2020-56-2-144-156

Поступила в редакцию 22.10.2019
Received 22.10.2019

Н. П. Прохоров

Белорусский государственный университет, Минск, Беларусь

ВЕРОЯТНОСТНЫЙ И ДЕТЕРМИНИРОВАННЫЙ АНАЛОГИ АЛГОРИТМА МИЛЛЕРА – РАБИНА ДЛЯ ИДЕАЛОВ КОЛЕЦ ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЭЛЕМЕНТОВ КОНЕЧНЫХ РАСШИРЕНИЙ ПОЛЯ $\mathbb{Q}$

Аннотация. Получены критерии простоты для идеалов колец целых алгебраических элементов конечных расширений поля $\mathbb{Q}$, которые являются аналогами критериев Миллера и Эйлера простоты для кольца целых чисел. Также получены их усиленные аналоги в предположении расширенной гипотезы Римана. Разработаны арифметические и модулярные операции для идеалов колец целых алгебраических элементов расширений поля $\mathbb{Q}$. С помощью указанных критериев предложены полиномиальные вероятностные и детерминированные алгоритмы решения задачи тестирования на простоту в кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$.

Ключевые слова: конечное расширение, кольцо целых алгебраических элементов, идеал, простота идеала, тестирование на простоту, критерий Миллера, критерий Эйлера, тест Миллера – Рабина

Для цитирования. Прохоров, Н. П. Вероятностный и детерминированный аналоги алгоритма Миллера – Рабина для идеалов колец целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ / Н. П. Прохоров // Вес. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. – 2020. – Т. 56, № 2. – С. 144–156. https://doi.org/10.29235/1561-2430-2020-56-2-144-156

Nikolai P. Prochorov

Belarusian State University, Minsk, Belarus

PROBABILISTIC AND DETERMINISTIC ANALOGUES OF THE MILLER – RABIN ALGORITHM FOR IDEALS OF RINGS OF INTEGER ALGEBRAIC ELEMENTS OF FINITE EXTENSIONS OF THE FIELD $\mathbb{Q}$

Abstract. In this paper, we obtained the primality criteria for ideals of rings of integer algebraic elements of finite extensions of the field $\mathbb{Q}$, which are analogues of Miller and Euler's primality criteria for rings of integers. Also advanced analogues of these criteria were obtained, assuming the extended Riemann hypothesis. Arithmetic and modular operations for ideals of rings of integer algebraic elements of finite extensions of the field $\mathbb{Q}$ were elaborated. Using these criteria, the polynomial probabilistic and deterministic algorithms for the primality testing in rings of integer algebraic elements of finite extensions of the field $\mathbb{Q}$ were offered.

Keywords: finite extension, ring of integer algebraic elements, ideal, primality of ideal, primality testing, Miller criterion, Euler criterion, Miller – Rabin test

For citation. Prochorov N. P. Probabilistic and deterministic analogues of the Miller – Rabin algorithm for ideals of rings of integer algebraic elements of finite extensions of the field $\mathbb{Q}$. *Vestsi Natsyianal'nai akademii navuk Belarusi. Seryia fizika-matematychnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics series*, 2020, vol. 56, no. 2, pp. 144–156 (in Russian). https://doi.org/10.29235/1561-2430-2020-56-2-144-156

Введение. Алгоритмическая теория чисел начала активно развиваться со второй половины XX в., что, в частности, связано с развитием информатики и криптографии, а также применениями теории чисел в указанных сферах. В частности, был получен ряд существенных результатов, связанных со свойствами целых простых чисел и способами проверки их на простоту.

В 1976 г. Г. Миллером [1] был предложен критерий и построен первый полиномиальный алгоритм тестирования чисел на простоту в предположении верности расширенной гипотезы Римана. Несколько позже алгоритм был модифицирован Э. Бахом [2]. Наконец в 1980 г. М. Рабин [3] на основе критерия Миллера предложил полиномиальный вероятностный алгоритм тестирования чисел на простоту, который в настоящее время является самым эффективным вероятностным безусловным алгоритмом тестирования на простоту, позволяющим определять с вероятностью

близкой к 1 при достаточном числе итераций является ли число простым. Также существует ряд других алгоритмов проверки на простоту, например тест Соловея – Штрассена [4], тест Адлемана – Померанса – Румели [5], являющийся одним из наиболее эффективных детерминированных алгоритмов проверки на простоту. В 2002 г. было конструктивно доказано [6], что задача проверки на простоту принадлежит классу $\mathcal{P}$. Данные результаты представляют большой интерес как с теоретической, так и практической точки зрения, так как при генерации ключей ряда криптосистем (например, RSA, Рабина, Блюма – Гольдвассер) требуется уметь быстро решать задачи проверки числа на простоту.

В настоящей работе рассматриваются вопросы о построении критериев простоты и алгоритмов проверки на простоту в более общих алгебраических структурах, а именно: исследуется задача тестирования на простоту идеалов колец целых алгебраических элементов конечных расширений $\mathbb{Q}$.

Вопросы о простых идеалах колец целых алгебраических элементов ранее рассматривались в ряде работ. Например, в [7] приводится необходимое и достаточное условие простоты, в [8] – построены критерии простоты в квадратичных кольцах, в [9] – алгоритмы проверки на простоту в квадратичных факториальных кольцах. В статьях [10, 11] исследованы свойства аналогов чисел Кармайкла в кольцах целых алгебраических элементов. Наконец в 2016 г. в [12] было доказано, что задача тестирования идеалов в произвольных кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ полиномиально разрешима.

Тем не менее полученный алгоритм носит скорее теоретический характер, так как основан на AKS-алгоритме для целых чисел. Более того, в настоящее время не существует эффективных и универсальных алгоритмов тестирования идеалов на простоту в соответствующих кольцах. Исходя из этого, целью данной работы является построение новых критериев простоты идеалов, а также основанных на них алгоритмов.

В первом разделе работы вводятся необходимые понятия об идеалах колец целых алгебраических элементов конечных расширений $\mathbb{Q}$, а также исследуются арифметика и способы представления элементов соответствующих колец. Во втором – исследуются алгоритмические примитивы для идеалов колец целых алгебраических элементов конечных расширений $\mathbb{Q}$, а также приводятся необходимые и достаточные условия их простоты. В третьем – выводятся аналоги критериев Миллера и Эйлера для идеалов, а также их усиленные версии в классе факториальных колец в предположении расширенной гипотезы Римана, в качестве следствий из критериев получаются вероятностные и детерминированные алгоритмы тестирования идеалов на простоту.

1. Постановка задачи. Будем считать, что $K \subset \mathbb{C}$ – конечное расширение $\mathbb{Q}$, $\mathcal{O}_K$ – кольцо целых алгебраических элементов K, под базисом K будем понимать базис K как векторного пространства над $\mathbb{Q}$, под нормой элемента α расширения K будем понимать абсолютное значение его нормы и обозначать ее $\mathrm{Nm}(\alpha)$.

Под идеалом $\mathfrak{n}$ кольца $\mathcal{O}_K$ будем понимать подкольцо $\mathcal{O}_K$ такое, что для любого $n \in \mathfrak{n}$ и $m \in \mathcal{O}_K$ выполнено $nm \in \mathfrak{n}$. Для идеалов можно ввести понятия умножения, делимости, НОДа, простоты по аналогии с целыми числами. Известно, что любой идеал можно представить в виде произведения простых идеалов с точностью до перестановки слагаемых, т. е. выполнен аналог основной теоремы арифметики.

Будем говорить, что $a \equiv b (\mathrm{mod}\, \mathfrak{n})$ если $a - b \in \mathfrak{n}$ или, другими словами, $\mathfrak{n}$ делит $a - b$. Введем $\mathcal{O}_{K,\mathfrak{n}} = \mathcal{O}_K / \mathfrak{n}$ и $\mathcal{O}^{\times}_{K,\mathfrak{n}} = (\mathcal{O}_K / \mathfrak{n})^{\times}$. Пусть $\mathrm{Nm}(\mathfrak{n}) = |\mathcal{O}_{K,\mathfrak{n}}|$ и $\varphi_K(\mathfrak{n}) = |\mathcal{O}^{\times}_{K,\mathfrak{n}}|$.

Главным идеалом будем называть идеал $\mathfrak{n} = (n) = n\mathcal{O}_K$. Отметим, что в случае факториального $\mathcal{O}_K$ любой идеал является главным, а значит, может быть задан с помощью одного элемента $\mathcal{O}_K$.

Для любого простого идеала $\mathfrak{p}$ нечетной нормы и $a \in \mathcal{O}^{\times}_{K,\mathfrak{p}}$ введем символ Лежандра $\left[\frac{a}{\mathfrak{p}}\right]$, равный 1, если a – квадратичный вычет по модулю $\mathfrak{p}$, и равный –1, если a – квадратичный невычет по модулю $\mathfrak{p}$. Для любого нетривиального идеала $\mathfrak{n}$ нечетной нормы кольца $\mathcal{O}_K$ и $a \in \mathcal{O}^{\times}_{K,\mathfrak{n}}$ может быть введен символ Якоби $\left[\frac{a}{\mathfrak{n}}\right]$, равный произведению символов Лежандра

$$\left[\frac{a}{\mathfrak{n}}\right]=\prod_{i=1}^{k}\left[\frac{a}{\mathfrak{p}_i}\right], \tag{1}$$

где $\mathfrak{n}=\mathfrak{p}_1\ldots\mathfrak{p}_k$, $\mathfrak{p}_i$ – простые идеалы $\mathcal{O}_K$.

Все необходимые понятия могут быть найдены в [7].

Под задачей тестирования идеала на простоту будем понимать следующую. Пусть зафиксировано некоторое кольцо $\mathcal{O}_K$, на вход подается идеал $\mathfrak{n}$, требуется определить, является ли он простым.

Далее исследуем некоторые арифметические и модулярные операции над элементами колец целых алгебраических элементов и сложности их выполнения.

Пусть $f(L)$, $g(L)$ – две различные функции натурального аргумента L. Будем писать $f(L)=\tilde{O}\big(g(L)\big)$, если существует положительная функция $h(L)$, такая что $f(L)\le h(L)g(L)$ для любых $L\in\mathbb{N}$, и $h(L)=O\big(\log g(L)\log\log g(L)\big)$. Данное обозначение вводится в связи с известной оценкой сложности перемножения двух натуральных чисел по алгоритму Шёнхаге – Штрассена. Любое положительное действительное число C будет называться эффективно вычислимой константой (или просто константой), если оно зависит только от инвариантов поля K (например, степени, дискриминанта Δ_K, интегрального базиса, системы фундаментальных единиц) и существует алгоритм нахождения данного числа.

Определение 1. *Целым базисом в $\mathcal{O}_K$ будем называть такой базис $E=\{e_1,\ldots,e_n\}$ поля, что любой элемент $\mathcal{O}_K$ представим в виде линейной комбинации с целыми рациональными коэффициентами.*

Утверждение 1 [7]. *Целый базис существует в любом конечном расширении $\mathbb{Q}$.*

Во всех алгоритмах элементы кольца будут кодироваться как коэффициенты в разложении по фиксированному целому базису. Инварианты поля K будем считать константами.

Определение 2. *Пусть $E=\{e_1,\ldots,e_n\}$ – фиксированный целый базис в K и $\alpha=\sum_{i=1}^{n}\alpha_i e_i\in\mathcal{O}_K$, $\alpha_i\in\mathbb{Z}$. Абсолютным значением α будем называть*

$$|\alpha|_\infty=\max_{i=1,n}|\alpha_i|. \tag{2}$$

Таким образом, логарифм абсолютного значения характеризует длину записи элемента $\mathcal{O}_K$.

Далее под множеством $\mathcal{O}_K^*$ будем понимать множество $\mathcal{O}_K\setminus\{0\}$.

Определение 3. *Для любого $a\in\mathcal{O}_K^*$ обозначим через $\overline{a}\in\mathcal{O}_K^*$ сопряженный элемент, определяемый как $\overline{a}=\mathrm{Nm}(a)/a$.*

Далее предполагаем, что элементы заданы с помощью коэффициентов своего разложения в целый базис $\mathcal{O}_K$.

Утверждение 2. *Пусть $a,b\in\mathcal{O}_K^*$ и $|a|_\infty\le L,|b|_\infty\le L$, тогда $a+b$, ab, b/a (включая проверку условия $a\mid b$), $\mathrm{Nm}(a)$, $\overline{a}$ могут быть вычислены за $\tilde{O}(\log L)$ бинарных операций.*

Доказательство. Рассмотрим произвольные элементы $a=\sum_{i=1}^{n}\alpha_i e_i$, $b=\sum_{i=1}^{n}\beta_i e_i\in\mathcal{O}_K$, такие что $|a|_\infty\le L,|b|_\infty\le L$. Утверждение для суммы $a+b$ очевидно. Используя алгоритм Шёнхаге – Штрассена быстрого перемножения чисел, нетрудно получить необходимое утверждение для произведения ab. Известно, что $\mathrm{Nm}(a)=|\det A|$, где $A=(a_{ij})\in\mathbb{Z}^{n\times n}$ – матрица, такая что $ae_i=\sum_{j=1}^{n}a_{ij}e_j$ $(i=1,\ldots,n)$. Определитель $\det A$ может быть найден с помощью операций сложения и умножения за $\tilde{O}(\log L)$ бинарных операций. Пусть $\overline{a}=\sum_{i=1}^{n}x_i e_i$, где x_i – неизвестные целые коэффициенты. Пусть

$$\mathrm{Nm}(a)=\sum_{i,j=1}^{n}\alpha_i x_j e_i e_j=\sum_{k=1}^{n}\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i x_j\alpha_k^{i,j}\right)e_k, \tag{3}$$

где $e_ie_j=\sum_{k=1}^{n}\alpha_k^{i,j}e_k$, тогда выполнено соотношение

$$H(x_1, x_2, \ldots, x_n)^T = \left(\mathrm{Nm}(a), 0, \ldots, 0\right)^T, \tag{4}$$

где H – матрица элементов $h_{ij} \in \mathbb{Z}$ $(i, j = 1, \ldots, n)$, такая что $h_{ij} = O(L)$ $(i, j = 1, \ldots, n)$. Тогда существует константа D, такая что $\mathrm{Nm}(a) \le D\,|a|_\infty^n$. Следовательно, решение $(x_1, x_2, \ldots, x_n)^T$ может быть найдено за $\tilde{O}(\log L)$ бинарных операций. Пусть $b\overline{a} = \sum_{i=1}^n y_i e_i$, $y_i \in \mathbb{Z}$. Тогда $b/a = \dfrac{b\overline{a}}{\mathrm{Nm}(a)}$, условие $a \mid b$ эквивалентно условию $\mathrm{Nm}(a) \mid y_i$ для любых $i = 1, \ldots, n$. Элемент b/a может быть определен за $\tilde{O}(\log L)$ с помощью произведения в $\mathcal{O}_K$ и деления целых рациональных чисел.

Замечание 1. В доказательстве утверждения было показано, что существует константа D, такая что $\mathrm{Nm}(a) \le D\,|a|_\infty^n$ для любого $a \in \mathcal{O}_K$. Из предыдущего утверждения и правила Крамера следует, что существуют константы R и q, такие что $|\overline{a}|_\infty \le RL^q$ для любого $a \in \mathcal{O}_K$, если $|a|_\infty \le L$.

Утверждение 3. *Существует константа M, такая что для любых $a, m \in \mathcal{O}_K^*$ может быть найдено $z \in \mathcal{O}_K$, удовлетворяющее условию $a \equiv z (\mathrm{mod}\, m)$ и $|z|_\infty \le M\,|m|_\infty$. Если $|a|_\infty \le L, |m|_\infty \le L$, то такой элемент z может быть определен за $\tilde{O}(\log L)$ бинарных операций.*

Доказательство. Пусть $a = \sum_{i=1}^n a_i e_i$, $m = \sum_{i=1}^n m_i e_i \in \mathcal{O}_K^*$. Тогда получаем

$$\frac{a}{m} = \frac{a\overline{m}}{\mathrm{Nm}(m)} = \frac{1}{\mathrm{Nm}(m)} \sum_{i=1}^n b_i e_i = \sum_{i=1}^n \left\lfloor \frac{b_i}{\mathrm{Nm}(m)} \right\rfloor e_i + \sum_{i=1}^n \frac{b_i'}{\mathrm{Nm}(m)} e_i, \tag{5}$$

где $b_i' \in \mathbb{Z}$, $|b_i'| < \mathrm{Nm}(m)$, $i = 1, \ldots, n$. Так как $a\overline{m} \equiv \sum_{i=1}^n b_i' e_i \left(\mathrm{mod}\, \mathrm{Nm}(m)\right)$, имеем $\overline{m} \mid \sum_{i=1}^n b_i' e_i$. Тогда $a \equiv z (\mathrm{mod}\, m)$, где $z = \dfrac{1}{m} \sum_{i=1}^n b_i' e_i$. Так как

$$z = \frac{1}{\mathrm{Nm}(m)} \sum_{k=1}^n e_k \left(\sum_{i,j=1}^n b_i' m_j \alpha_k^{i,j} \right), \tag{6}$$

получаем

$$|z|_\infty = \max_{k=1,n} \left| \frac{1}{\mathrm{Nm}(m)} \sum_{i,j=1}^n b_i' m_j \alpha_k^{i,j} \right| < \max_{k=1,n} \sum_{i,j=1}^n |m_j \alpha_k^{i,j}| \le$$

$$\le |m|_\infty \max_{k=1,n} \sum_{i,j=1}^n |\alpha_k^{i,j}| = M\,|m|_\infty. \tag{7}$$

Предположим, что $|a|_\infty \le L, |m|_\infty \le L$. Тогда $|\overline{m}|_\infty \le RL^q$, где q и R – эффективно вычислимые константы. Так как существует константа D, такая что $\mathrm{Nm}(m) \le D\,|m|_\infty^n$, числа b_i, b_i' могут быть найдены за $\tilde{O}(\log L)$ бинарных операций. Поэтому элемент z может быть определен в K по формуле (6) с использованием не более $\tilde{O}(\log L)$ бинарных операций.

Следствие 1. *Пусть $k \in \mathbb{N}$, и для $a, b, m \in \mathcal{O}_K^*$ выполнено $|a|_\infty \le L$, $|b|_\infty \le L$, $|m|_\infty \le L$. Элементы $z_1, z_2 \in \mathcal{O}_K$ такие, что $a + b \equiv z_1 (\mathrm{mod}\, m)$, $a^k \equiv z_2 (\mathrm{mod}\, m)$, $|z_1|_\infty \le M\,|m|_\infty$, $|z_2|_\infty \le M\,|m|_\infty$ могут быть определены за $\tilde{O}(\log L)$, $\tilde{O}(\log k \log L)$ бинарных операций соответственно.*

2. Операции над идеалами в кольцах целых алгебраических элементов. Далее будем считать, что $[K : \mathbb{Q}] = n$.

Определение 4. *Представление*

$$\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}} = \left\{ e_1 x_1 + \ldots + e_m x_m \mid x_i \in \mathbb{Z},\, i = \overline{1, m} \right\}, \tag{8}$$

где $E = \{e_1, \ldots, e_m\} \subset \mathcal{O}_K$ – базис $\mathfrak{a}$ как $\mathbb{Z}$-модуля, будем называть $\mathbb{Z}$ – представлением идеала $\mathfrak{a}$.

Далее для удобства будем полагать, что $m = n$.

Далее под $\mathbb{Z}$-представлением будем понимать матрицу $A \in \mathbb{Z}^{n\times n}$, такую что ее столбец под номером i – это коэффициенты разложения e_i в фиксированный целый базис $\mathcal{O}_K$.

В [13, 14] доказывается, что любой идеал имеет $\mathbb{Z}$-представление.

О п р е д е л е н и е 5. *Представление*

$$\mathfrak{a} = (a, \alpha)_2 = \{a\xi_1 + \alpha\xi_2 \mid \xi_1, \xi_2 \in \mathcal{O}_K\}, \tag{9}$$

где $a \in \mathbb{N}_0$, $\alpha \in \mathcal{O}_K$, *будем называть* 2*-представлением идеала* $\mathfrak{a}$.

В [13, 14] доказывается, что любой идеал имеет 2-представление.

Далее под 2-представлением будем понимать вектор $\mathbb{Z}^n$ – коэффициенты разложения α в целый базис и целое неотрицательное число a.

В [14] приведены полиномиальные алгоритмы перехода от 2-представления к $\mathbb{Z}$-представлению и обратно. К сожалению, несмотря на полиномиальность алгоритма, он может оказаться достаточно трудоемким.

Рассмотрим один важный частный случай $\mathbb{Z}$-представления.

О п р е д е л е н и е 6. *Будем говорить, что матрица* $A \in \mathbb{Z}^{n\times n}$ *записана в нормальной эрмитовой форме, если выполнены следующие условия:*

1) $m_{i,j} = 0$, *если* $i > j$;

2) $m_{i,j} > 0$ *для любого* i;

3) для любого $i < j$ *выполнено* $0 \le m_{i,j} < m_{i,i}$.

О п р е д е л е н и е 7. *Представлением идеала* $\mathfrak{a}$ *в нормальной эрмитовой форме будем называть такое его* $\mathbb{Z}$*-представление*

$$\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}}, \tag{10}$$

что соответствующая матрица является матрицей в эрмитовой нормальной форме.

В [13, 14] показывается, что каждый идеал может быть записан в нормальной эрмитовой форме, более того, такое представление единственно.

В статье [15] был получен полиномиальный алгоритм построения нормальной эрмитовой формы по $\mathbb{Z}$-представлению идеала.

С л е д с т в и е 2. *Таким образом, за полиномиальное время можно переходить от* $\mathbb{Z}$*-представления,* 2*-представления или представления в нормальной эрмитовой форме к любому из них.*

О п р е д е л е н и е 8. *Пусть дан идеал* $\mathfrak{a}$, *зафиксирован целый базис* E *кольца* $\mathcal{O}_K$ *и* $\mathbb{Z}$*-представление идеала* $\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}}$. *Тогда введем абсолютное значение идеала* $\mathfrak{a}$ *как*

$$|\mathfrak{a}|_\infty = \max_{i=\overline{1,n},\, j=\overline{1,n}} |a_{ij}|, \tag{11}$$

где $A = (a_{ij}) \in \mathbb{Z}^{n\times n}$ *– матрица, соответствующая указанному* $\mathbb{Z}$*-представлению.*

Нетрудно видеть, что логарифм абсолютного значения идеала характеризует количество памяти, необходимое для того, чтобы закодировать его $\mathbb{Z}$-представление.

В случае, когда кольцо $\mathcal{O}_K$ факториально, любой идеал является главным, а значит, любой идеал может быть задан с помощью порождающего его элемента. Поэтому в таких кольцах идеал, как и любой элемент, будет кодироваться в виде вектора $\mathbb{Z}^n$ коэффициентов разложения в целый базис кольца $\mathcal{O}_K$.

У т в е р ж д е н и е 4. *Пусть идеалы* $\mathfrak{a}$ *и* $\mathfrak{b}$ *заданы в виде нормальной эрмитовой формы и* $|\mathfrak{a}|_\infty, |\mathfrak{b}|_\infty \le L$, *тогда проверка указанных идеалов на равенство может быть выполнена за* $O(\log L)$ *бинарных операций.*

Д о к а з а т е л ь с т в о. Как было указано ранее, любой идеал однозначно задается своей нормальной эрмитовой формой. Таким образом, достаточно проверить на поэлементное равенство две целочисленные матрицы $n \times n$ с коэффициентами размера $O(L)$.

Утверждение 5. *Пусть идеал* $\mathfrak{a}$ *задан в виде* $\mathbb{Z}$*-представления и* $|\mathfrak{a}|_\infty \le L$, *тогда* $\mathrm{Nm}(\mathfrak{a})$ *может быть вычислено за* $\tilde{O}(\log L)$ *бинарных операций.*

Доказательство. Исходя из утверждения, описанного в [14], выполнено равенство $\mathrm{Nm}(\mathfrak{a}) = |\det(A)|$, где A – матрица, соответствующая $\mathbb{Z}$-представлению. Нетрудно видеть, что определитель целочисленной матрицы $n \times n$ с коэффициентами размера $O(L)$ может быть вычислен за указанное число операций.

Утверждение 6. *Пусть идеал* $\mathfrak{a}$ *задан в виде* $\mathbb{Z}$*-представления и* $|\mathfrak{a}|_\infty, |a|_\infty, |b|_\infty \le L$, *тогда проверка сравнения* $a \equiv b (\mathrm{mod}\, \mathfrak{a})$ *может быть выполнена за* $\tilde{O}(\log L)$ *бинарных операций.*

Доказательство. Пусть изначально $\mathfrak{a}$ задан в виде $\mathbb{Z}$-представления и $|\mathfrak{a}|_\infty, |a|_\infty, |b|_\infty \le L$. Требуется проверить делимость главного идеала $(a - b)$ на идеал $\mathfrak{a}$, что эквивалентно проверке включения главного идеала $(a - b)$ в идеал $\mathfrak{a}$. А это, в свою очередь, равносильно тому, что $a - b \in \mathfrak{a}$. То есть проверка сравнения сводится к проверке разложимости $a - b$ по базису идеала $\mathfrak{a}$, т. е. проверке разрешимости системы линейных уравнений $n \times n$ с коэффициентами размера $O(L)$. Нетрудно видеть, что это может быть сделано за $\tilde{O}(\log L)$ бинарных операций.

Утверждение 7. *Существует константа N, такая что для любого нетривиального идеала* $\mathfrak{n}$ *и* $a \in \mathcal{O}_K$ *найдется* $z \in \mathcal{O}_K$, *такое что* $z \equiv a (\mathrm{mod}\, \mathfrak{n})$ *и* $|z|_\infty \le N |\mathfrak{n}|_\infty^n$. *Если* $\mathfrak{n}$ *задан с помощью* $\mathbb{Z}$*-представления, причем* $|\mathfrak{n}|_\infty, |a|_\infty \le L$, *то такой элемент z может быть вычислен за* $\tilde{O}(\log L)$ *бинарных операций.*

Доказательство. Пусть $E = (e_1,...,e_n)$ – целый базис в $\mathcal{O}_K$, $\mathfrak{n} = (\omega_1, \ldots, \omega_n)_{\mathbb{Z}}$ – $\mathbb{Z}$-представление идеала $\mathfrak{n}$. Пусть далее

$$a = \sum_{i=1}^{n} \alpha_i e_i, \quad \theta = \mathrm{НОК}\big(\mathrm{Nm}(\omega_1), \ldots, \mathrm{Nm}(\omega_n)\big).$$

Нетрудно видеть, что $\theta \in \mathfrak{n}$, вследствие чего $\theta \equiv 0 (\mathrm{mod}\, \mathfrak{n})$. Отсюда следует, что $a \equiv a - \beta\theta (\mathrm{mod}\, \mathfrak{n})$ для любого $\beta \in \mathcal{O}_K$.

Положим $\beta = \sum_{i=1}^{n} \beta_i e_i$, где $\alpha_i = \theta\beta_i + r_i$, $r_i < \theta, i = \overline{1,n}$, а также $z = a - \beta\theta$. Тогда

$$|z|_\infty = \max_{i=1,n} |r_i| \le |\theta| \le \prod_{i=1}^{n} \mathrm{Nm}(\omega_i) \le D^n \prod_{i=1}^{n} |\omega_i|_\infty \le D^n |\mathfrak{n}|_\infty^n = N |\mathfrak{n}|_\infty^n . \tag{12}$$

Нетрудно видеть, что рассмотренные операции могут быть выполнены за $\tilde{O}(\log L)$ бинарных операций.

Следствие 3. *Пусть* $k \in \mathbb{N}$ *и* $a, b \in \mathcal{O}_K^*$, $\mathfrak{n}$ – *нетривиальный идеал, заданный с помощью* $\mathbb{Z}$*-представления. Пусть выполнено* $|a|_\infty \le L$, $|b|_\infty \le L$, $|\mathfrak{n}|_\infty \le L$. *Элементы* z_1, $z_2 \in \mathcal{O}_K$ *такие, что* $a + b \equiv z_1 (\mathrm{mod}\, \mathfrak{n})$, $a^k \equiv z_2 (\mathrm{mod}\, \mathfrak{n})$, $|z_1|_\infty \le N |\mathfrak{n}|_\infty^n$, $|z_2|_\infty \le N |\mathfrak{n}|_\infty^n$ *могут быть определены за* $\tilde{O}(\log L)$, $\tilde{O}(\log k \log L)$ *бинарных операций соответственно.*

Замечание 2. Отметим, что все указанные операции могут быть выполнены за полиномиальное время в случае, когда идеалы заданы с помощью одного из представлений: $\mathbb{Z}$-представление, 2-представление, нормальная эрмитовая форма; в силу того, что из одного представления может быть получено другое за полиномиальное время.

Далее рассмотрим некоторые необходимые и достаточные условия простых идеалов в $\mathcal{O}_K$. Для удобства обозначим через $\mathcal{P}_K$ множество простых идеалов $\mathcal{O}_K$, $P_{1,K}$ – множество простых идеалов нечетной нормы, $P_{2,K}$ – множество простых идеалов четной нормы. Пусть также $\mathcal{T}_K = \{\varepsilon x \mid x \in \mathbb{Z}, \varepsilon \in \mathcal{O}_K^\times\}$, $\mathcal{Q}_K = \mathcal{O}_K \setminus \mathcal{T}_K$.

Приведем следующее достаточное условие простоты.

Утверждение 8. *Пусть* $\mathfrak{p}$ – *идеал и* $\mathrm{Nm}(\mathfrak{p})$ – *простое в* $\mathbb{Z}$, *тогда* $\mathfrak{p}$ – *простой идеал.*

Доказательство. Предположим, что $\mathfrak{p}$ – не простой, тогда $\mathfrak{p} = \mathfrak{m}\mathfrak{n}$, где $\mathfrak{m}, \mathfrak{n} \neq (1)$. Значит, $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{n})\mathrm{Nm}(\mathfrak{m})$. Противоречие.

Отметим, что данное утверждение во многих кольцах не является необходимым. В [7] приводится следующее необходимое условие простоты.

У т в е р ж д е н и е 9. *Пусть* $\mathfrak{p}$ – *простой идеал, тогда существует* q – *простое в* $\mathbb{Z}$, *что* $\mathrm{Nm}(\mathfrak{p}) = q^f$, *где* $f \in \mathbb{N}$.

Отметим, что данное необходимое условие ни в каком $\mathcal{O}_K$ не является достаточным.

З а м е ч а н и е 3. Также известен следующий критерий для случая квадратичных колец [12].

Пусть $d \in \mathbb{Z} \setminus \{1\}$ – целое число, свободное от квадратов, $K = \mathbb{Q}(\sqrt{d})$ и $\mathcal{O}_K$ – факториально. Тогда верны следующие утверждения:

1) $p \in \mathcal{Q}_K$ простое тогда и только тогда, когда $\mathrm{Nm}(p)$ простое в $\mathbb{Z}$;

2) $p \in \mathcal{T}_K \setminus \{2\varepsilon \mid \varepsilon \in \mathcal{O}_K^\times\}$ и $(p) = (p^*)$, где $p^* \in \mathbb{Z}$, значит, p простое тогда и только тогда, когда $\left(\frac{\Delta_K}{p^*}\right) = -1$;

3) $p \in \{2\varepsilon \mid \varepsilon \in \mathcal{O}_K^\times\}$ простое тогда и только тогда, когда $d \equiv 5 (\mathrm{mod}\ 8)$.

З а м е ч а н и е 4. Отметим, что число идеалов с фиксированной нормой конечно. Действительно, пусть $\mathfrak{n}$ – идеал $\mathcal{O}_K$, такой что $\mathrm{Nm}(\mathfrak{n}) = N$, тогда получаем, что $\mathfrak{n}$ делит (N). В свою очередь (N) имеет конечное число делителей-идеалов.

Из данного замечания и утверждения 9 следует, что множество $\mathcal{P}_{2,K}$ конечно, и норма любого идеала из $\mathcal{P}_{2,K}$ является степенью двойки.

3. Критерии простоты идеалов. Докажем аналог критерия Эйлера [4] для идеалов колец целых алгебраических элементов конечных расширений $\mathbb{Q}$.

Т е о р е м а 1. *Пусть* $\mathfrak{n}$ – *нетривиальный идеал нечетной нормы. Тогда* $\mathfrak{n}$ *является простым в* $\mathcal{O}_K$ *тогда и только тогда, когда для любого* $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$ *выполнено сравнение*

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\,\mathfrak{n}).$$

Д о к а з а т е л ь с т в о. Докажем необходимость. Пусть $\mathfrak{n}$ является нетривиальным простым идеалом нечетной нормы. Рассмотрим произвольный элемент $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$. Таким образом, требуется доказать, что a – квадратичный вычет по модулю $\mathfrak{n}$ тогда и только тогда, когда выполнено равенство

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv 1 (\mathrm{mod}\,\mathfrak{n}). \tag{13}$$

Так как идеал $\mathfrak{n}$ простой, то $\mathcal{O}_{K,\mathfrak{n}}$ является полем, соответственно группа $\mathcal{O}_{K,\mathfrak{n}}^\times$ циклична, и в ней существует первообразный корень g. Так как $\mathrm{Nm}(\mathfrak{n})$ нечетно, то a является квадратичным вычетом по модулю $\mathfrak{n}$ тогда и только тогда, когда существует четное число $t \in \{0,1,\ldots,\mathrm{Nm}(\mathfrak{n})-1\}$, такое что $a \equiv g^t (\mathrm{mod}\,\mathfrak{n})$. Последнее равносильно соотношению (13).

Докажем достаточность. Пусть $\mathfrak{n}$ – нетривиальный идеал нечетной нормы, такой что для любого элемента $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$ выполнено

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\,\mathfrak{n}). \tag{13′}$$

Рассмотрим разложение идеала $\mathfrak{n}$ на простые сомножители – $\mathfrak{n} = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$, где $\mathfrak{p}_i$ – простые идеалы нечетной нормы и $\alpha_i \in \mathbb{N}$. Пусть $\mathrm{Nm}(\mathfrak{p}_j) = q_j^{f_j}$, где q_j – простое в $\mathbb{Z}$. Возможны 2 следующих случая.

С л у ч а й 1. Существует $j \in \{1,\ldots,r\}$, такое что $\alpha_j > 1$. Пусть $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$ – элемент порядка $q_j l$ (такой элемент существует, исходя из аналога китайской теоремы об остатках для идеалов и теоремы Коши для абелевых групп [7]). Согласно соотношению (13′), имеем $q_j \mid \mathrm{Nm}(N) - 1$, что невозможно.

Случай 2. Пусть $\alpha_i = 1$ для любого $i \in \{1,\dots,r\}$, $r \geq 2$. Пусть $b \in \mathcal{O}^{\times}_{K,\mathfrak{p}_1}$ – произвольный квадратичный невычет (такой существует, так как можно считать, что $\mathrm{Nm}(\mathfrak{p}_1) \geq 3$). Тогда существует элемент $a \in \mathcal{O}^{\times}_{K,\mathfrak{n}}$ такой, что выполнено $a \equiv b(\mathrm{mod}\mathfrak{p}_1)$, $a \equiv 1(\mathrm{mod}\mathfrak{p}_2 \dots \mathfrak{p}_r)$. Значит, $\left[\frac{a}{\mathfrak{n}}\right] = -1$, поэтому $a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv -1(\mathrm{mod}\mathfrak{n})$. Но последнее утверждение противоречит тому, что $a \equiv 1(\mathrm{mod}\mathfrak{p}_2)$.

Таким образом, мы показали, что идеал $\mathfrak{n}$ является простым в $\mathcal{O}_K$.

Следствие 4. *Исходя из результата* [16] *символ Якоби может быть вычислен за полиномиальное время. Соответственно на основе данного критерия и результатов разделов* 2, 3 *можно построить вероятностный полиномиальный тест, основанный на выборе случайного* $a \in \mathcal{O}^{*}_{K}$ *и проверки сравнения*

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right](\mathrm{mod}\mathfrak{n}).$$

Из теоремы Лагранжа очевидным образом следует, что вероятность успеха для составного идеала $\mathfrak{n}$ *на одной итерации такого теста не меньше* 1/2, *так как множество элементов* $a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right](\mathrm{mod}\mathfrak{n})$ *образует подгруппу* $\mathcal{O}^{\times}_{K,\mathfrak{n}}$.

Проводя l *итераций теста, можно определить простоту* N *с вероятностью не менее* $1 - 2^{-l}$. *Данный алгоритм обобщает результат статьи* [4].

Далее докажем аналог критерия Миллера [1].

Теорема 2. *Пусть* $\mathfrak{n}$ *– нетривиальный идеал нечетной нормы. Тогда следующие утверждения эквивалентны:*

1) $\mathfrak{n}$ *простой идеал;*

2) $\forall a, (a,\mathfrak{n}) = 1$, $a^u \not\equiv 1(\mathrm{mod}\mathfrak{n}) : \exists k \in \{0,\dots,t-1\}$, *такое что* $a^{2^k u} \equiv -1(\mathrm{mod}\mathfrak{n})$, *где* $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$, $(u,2) = 1$.

Доказательство. Докажем необходимость. Пусть $\mathfrak{n}$ является нетривиальным простым идеалом $\mathcal{O}_K$ нечетной нормы. Нетрудно видеть, что тогда $\varphi_K(\mathfrak{n}) = \mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$, $(u,2) = 1$. Возьмем произвольный элемент $a \in \mathcal{O}_K$, такой что $(a,\mathfrak{n}) = 1$ и $a^u \not\equiv 1(\mathrm{mod}\mathfrak{n})$. Исходя из аналога теоремы Эйлера, получаем, что верно сравнение $a^{\varphi_K(\mathfrak{n})} \equiv a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv a^{2^t u} \equiv 1(\mathrm{mod}\mathfrak{n})$. Таким образом,

$$(a^u - 1)(a^u + 1)(a^{2u} + 1)\dots\left(a^{2^{t-1}u} + 1\right) \equiv 0(\mathrm{mod}\mathfrak{n}). \tag{14}$$

Так как $a^u - 1 \not\equiv 0(\mathrm{mod}\mathfrak{n})$, то из соотношения (14) следует существование такого числа $k \in \{0,\dots,t-1\}$, что $a^{2^k u} \equiv -1(\mathrm{mod}\mathfrak{n})$.

Докажем достаточность. Предположим, что $\mathfrak{n}$ не является простым идеалом. Рассмотрим разложение идеала $\mathfrak{n}$ в произведение простых сомножителей: $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, где $\mathfrak{p}_i$ – различные простые идеалы нечетной нормы, $\alpha_i \in \mathbb{N}$. Пусть также $\mathrm{Nm}(\mathfrak{p}_j) = q_j^{f_j}$, где q_j – простое в $\mathbb{Z}$.

Возможны 2 случая.

Случай 3. Существует $j \in \{1,\dots,r\}$, такое что $\alpha_j > 1$. Существует $a \in \mathcal{O}^{\times}_{K,\mathfrak{n}}$ порядка $q_j l$. Так как $u \not\equiv 0(\mathrm{mod}q_j)$, то $a^u \not\equiv 1(\mathrm{mod}\mathfrak{n})$. Следовательно, существует число $k \in \{1,\dots,t-1\}$, такое что выполнено сравнение $a^{2^{k+1}u} \equiv 1(\mathrm{mod}\mathfrak{n})$. Значит, $2^{k+1}u \equiv 0(\mathrm{mod}q_j)$. Из последнего сравнения следует, что $\mathrm{Nm}(\mathfrak{n}) - 1 \equiv 0(\mathrm{mod}q_j)$, что невозможно.

Случай 4. Предположим $\alpha_j = 1$ для любого $j \in \{1,\ldots,r\}$, $r \geq 2$. Так как $\mathcal{O}_{K,\mathfrak{n}}^{\times} \cong \mathcal{O}_{K,\mathfrak{p}_1}^{\times} \times \ldots \times \mathcal{O}_{K,\mathfrak{p}_r}^{\times}$ и элемент –1 имеет порядок 2 в каждой группе $\mathcal{O}_{K,\mathfrak{p}_j}^{\times}$, то существует по крайней мере $2^r - 1 \geq 3$ элементов $\mathcal{O}_{K,\mathfrak{n}}^{\times}$ порядка 2. Пусть $a \not\equiv \pm 1 (\mathrm{mod}\mathfrak{n})$ является произвольным элементом порядка 2 в группе $\mathcal{O}_{K,\mathfrak{n}}^{\times}$. Так как число *u* нечетно, то $a^u = a \not\equiv \pm 1(\mathrm{mod}\mathfrak{n})$. Таким образом, существует $k \in \{0,\ldots,t-1\}$ такое, что верно $a^{2^k u} \equiv -1(\mathrm{mod}\mathfrak{n})$. Последнее сравнение невозможно, так как $a^u \not\equiv \pm 1(\mathrm{mod}\mathfrak{n})$ и *a* имеет порядок 2 в $\mathcal{O}_{K,\mathfrak{n}}^{\times}$. Во всех случаях было получено противоречие, следовательно, идеал $\mathfrak{n}$ является простым.

Замечание 5. На основе данного критерия и результатов разделов 2, 3 можно построить вероятностный полиномиальный тест, основанный на выборе случайного $a \in \mathcal{O}_K^*$ и проверки условия теоремы. Аналогично результатам, полученным в [3] и [9], можно показать, что вероятность успеха на одной итерации такого алгоритма не меньше 1/2, а значит, проводя *l* итераций теста, можно определить простоту *N* с вероятностью не менее $1 - 2^{-l}$. Отметим, что данный алгоритм обобщает результат статьи [3].

Далее будем считать, что $\mathcal{O}_K$ факториально, в частности, любой идеал $\mathcal{O}_K$ является главным.

Далее рассмотрим приложения расширенной гипотезы Римана к рассматриваемым вопросам.

Определение 9. *Характером Дирихле абелевой группы G будем называть гомоморфизм* $\chi : G \to \mathbb{C}^*$.

Рассмотрим характер ξ группы $\mathcal{O}_{K,\mathfrak{n}}^{\times}$. Его можно продолжить на всю группу $\mathcal{O}_K^*$ по правилу $\psi(x) = 0$, если $(x,\mathfrak{n}) \neq 1$; $\psi(x) = \xi(x \mathrm{mod}\mathfrak{n})$, если $(x,\mathfrak{n}) = 1$. Нетрудно видеть, что ψ – характер $\mathcal{O}_K^*$. Характер будем называть нетривиальным, если его образ не является тривиальной группой.

Определение 10. *L-функция Гекке, ассоциированная с характером* $\chi : \mathcal{O}_K \to \mathbb{C}^*$, *определяется как непрерывное продолжение на* $\mathbb{C}$ *функции*

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{(\mathrm{Nm}(\mathfrak{a}))^s}, \quad s \in \mathbb{C}, \tag{15}$$

где сумма справа берется по всем ненулевым идеалам $\mathfrak{a}$.

Следующая версия расширенной гипотезы Римана (ERH) предполагается верной для доказательства аналога теоремы Анкени.

Гипотеза [2]. *Все L-функции Гекке не имеют нулей в полуплоскости* $\mathrm{Re}(z) > 1/2$ (*ERH*).

Классическая теорема Анкени [2, 17] гласит, что в предположении выполнимости ERH для любого нетривиального характера χ группы $\mathbb{Z}_N^*$ найдется $m \in \mathbb{N}$, $(m,N) = 1$, что $m \leq 2\log^2 N$ и $\chi(m) \neq 1$. В статье [2] аналог данной теоремы в предположении ERH был доказан для группы $\mathcal{O}_{K,N}^{\times}$.

Утверждение 10. *Предположим, что ERH выполнена;* χ *– нетривиальный характер Дирихле группы* $\mathcal{O}_{K,N}^{\times}$. *Тогда существует простой элемент* $p \in \mathcal{O}_K$, $(p,N) = 1$, *такой что* $\mathrm{Nm}(p) \leq 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right)$ *и* $\chi(N) \neq 1$.

Из него можно получить следующее следствие.

Утверждение 11. *Предположим, что ERH выполнена. Пусть G является конечной абелевой группой и* $\chi : \mathcal{O}_{K,N}^{\times} \to G$ *– нетривиальный гомоморфизм. Тогда существует простое* $p \in \mathcal{O}_K$, $(p,N) = 1$, *такое что* $\mathrm{Nm}(p) \leq 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right)$ *и* $\chi(p) \neq 1_G$.

Доказательство. Так как образ $\mathrm{Im}\chi$ отображения χ является нетривиальной подгруппой группы *G*, то можно определить нетривиальный гомоморфизм $\xi : \mathrm{Im}\chi \to \mathbb{C}^*$. Заметим, что $\xi \circ \chi : \mathcal{O}_{K,N}^{\times} \to \mathbb{C}^*$ является нетривиальным характером Дирихле. Понятно, что $\xi \circ \chi$ может быть расширен на все идеалы $\mathcal{O}_K$. Так как $\xi \circ \chi$ может быть рассмотрен в смысле определения 9, мы можем сделать вывод, что из утверждения 10 следует существование элемента $p \in \mathcal{O}_K$, $(p,N) = 1$, такого что

$$\mathrm{Nm}(p) \leq 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right) \tag{16}$$

и $(\xi \circ \chi)(p) \neq 1$.

Далее будем предполагать, что ERH выполнена.

Утверждение 12. *Пусть* $\mathfrak{p}$ *является нетривиальным простым идеалом нечетной нормы. Тогда сравнение*

$$x^{\mathrm{Nm}(\mathfrak{p})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{p}^2) \tag{17}$$

имеет не более $\mathrm{Nm}(\mathfrak{p})-1$ *решений относительно* $x \in \mathcal{O}^{\times}_{K,\mathfrak{p}^2}$.

Доказательство. Так как $\mathcal{O}_K$ факториально, то $\mathfrak{p}$ – главный идеал, пусть $\mathfrak{p} = (p)$. Рассмотрим сравнение $x^{\mathrm{Nm}(p)-1} \equiv 1 (\mathrm{mod}\, p)$. Из аналога теоремы Эйлера для идеалов следует, что оно выполнено для любого элемента $x \in \mathcal{O}^{\times}_{K,p}$, другими словами, данное сравнение имеет ровно $\mathrm{Nm}(p)-1$ решений относительно x.

Очевидно, что каждое решение сравнения $x^{\mathrm{Nm}(p)-1} \equiv 1 (\mathrm{mod}\, p^2)$ может быть записано в виде $a + pt$, $a \in \mathcal{O}^{\times}_{K,p}$, $t \in \mathcal{O}_{K,p}$, где a – это решение $x^{\mathrm{Nm}(p)-1} \equiv 1 (\mathrm{mod}\, p)$.

Применяя формулу бинома Ньютона к многочлену $P(t) = (a + pt)^{\mathrm{Nm}(p)-1} - 1$, получаем, что

$$\frac{a^{\mathrm{Nm}(p)-1} - 1}{p} + t\big(\mathrm{Nm}(p)-1\big)a^{\mathrm{Nm}(p)-2} \equiv 0 (\mathrm{mod}\, p). \tag{18}$$

Заметим, что данное сравнение является линейным относительно t, а значит, имеет единственное решение при фиксированном a, так как $\Big(\big(\mathrm{Nm}(p)-1\big)a^{\mathrm{Nm}(p)-2}, p\Big) = 1$.

Таким образом, сравнение $x^{\mathrm{Nm}(p)-1} \equiv 1 (\mathrm{mod}\, p^2)$ имеет не более $\mathrm{Nm}(p)-1$ решений относительно $x \in \mathcal{O}^{\times}_{K,p^2}$.

Теорема 3. *Предположим, что ERH выполняется. Пусть* $\mathfrak{n}$ *– нетривиальный идеал нечетной нормы. Тогда следующие утверждения эквиваленты:*

1) $\mathfrak{n}$ *является простым идеалом;*

2) $\forall a, (a, \mathfrak{n}) = 1, \mathrm{Nm}(a) \le 12 \log^2\Big(\Delta_K^2 \mathrm{Nm}(\mathfrak{n})\Big)$, $a^u \not\equiv 1 (\mathrm{mod}\, \mathfrak{n}) : \exists k \in \{0, \ldots, t-1\}$, *такое что* $a^{2^k u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$, *где* $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u, (u, 2) = 1$.

Доказательство. Так как $\mathcal{O}_K$ факториально, то $\mathfrak{n}$ – главный идеал, пусть $\mathfrak{n} = (N)$. Необходимость следует из теоремы 2.

Докажем достаточность. Предположим, что $N \in \mathcal{O}_K \setminus \mathcal{O}_K^{\times}$ – это составной элемент нечетной нормы, для которого утверждение (2) выполнено.

Предположим, что N не является свободным от квадратов, т. е. существует делитель $p \in \mathcal{P}_{2,K}$ элемента N, такой что N делится на p^2. Рассмотрим отображение $\chi : \mathcal{O}^{\times}_{K,p^2} \to \mathcal{O}^{\times}_{K,p^2}$, такое что для любого $a \in \mathcal{O}^{\times}_{K,N}$ выполнено $\chi(a) = a^{\mathrm{Nm}(p)-1}$. Нетрудно видеть, что χ является эндоморфизмом группы $\mathcal{O}_{K,p^2}$. Согласно утверждению 12, χ является нетривиальным. Применяя утверждение 11, получаем существование $\alpha \in \mathcal{O}^{\times}_{K,N}$, такого что $\mathrm{Nm}(\alpha) \le 12 \log^2\Big(\Delta_K^2 \mathrm{Nm}(N)\Big)$ и $\alpha^{\mathrm{Nm}(p)-1} \not\equiv 1 (\mathrm{mod}\, p^2)$.

Предположим, что $\alpha^{\mathrm{Nm}(N)-1} \equiv 1 (\mathrm{mod}\, N)$. Отсюда получаем сравнение $\alpha^{\mathrm{Nm}(N)-1} \equiv 1 (\mathrm{mod}\, p^2)$. Значит, выполнено

$$\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) \,|\, \mathrm{Nm}(N) - 1, \tag{19}$$

$$\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) \,|\, \varphi_K(p^2) = \mathrm{Nm}(p)\big(\mathrm{Nm}(p)-1\big). \tag{20}$$

Из этого следует соотношение $\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) \,|\, \mathrm{Nm}(p) - 1$, которое противоречит сравнению $\alpha^{\mathrm{Nm}(p)-1} \not\equiv 1 (\mathrm{mod}\, N)$.

Таким образом, $\alpha^{\mathrm{Nm}(N)-1} \not\equiv 1(\mathrm{mod}N)$ верно, и оно противоречит предположению. Следовательно, N является свободным от квадратов. Пусть $p,q \in \mathcal{P}_{2,K}$ – различные простые делители N. Обозначим через $v_2(n)$ максимальную степень двойки, делящую n. Без потери общности будем считать, что $v_2\left(\mathrm{Nm}(p)-1\right) \geq v_2\left(\mathrm{Nm}(q)-1\right)$. Введем следующий элемент $d \in \mathcal{O}_K$:

$$d = \begin{cases} pq, \text{если } v_2\left(\mathrm{Nm}(p)-1\right) = v_2\left(\mathrm{Nm}(q)-1\right), \\ p, \text{если } v_2\left(\mathrm{Nm}(p)-1\right) > v_2\left(\mathrm{Nm}(q)-1\right). \end{cases} \tag{21}$$

Рассмотрим отображение $\xi : \mathcal{O}_{K,N}^{\times} \to \mathcal{O}_{K,N}^{\times}$, такое что для любого $a \in \mathcal{O}_{K,N}^{\times}$ выполнено $\xi(a) = \left[\frac{a}{d}\right]$. Заметим, что ξ является нетривиальным эндоморфизмом группы $\mathcal{O}_{K,N}^{\times}$. Применяя утверждение 11, получаем существование $\alpha \in \mathcal{O}_{K,N}^{\times}$, такое что $\mathrm{Nm}(\alpha) \leq 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right)$ и $\left[\frac{\alpha}{d}\right] \equiv -1(\mathrm{mod}N)$. Пусть $\beta = \alpha^u$. Исходя из нечетности u, получаем $\left[\frac{\beta}{d}\right] = -1$, значит, $\beta \not\equiv 1(\mathrm{mod}d)$. Пусть j – минимальное число, такое что $\alpha^{2^j u} \equiv -1(\mathrm{mod}N)$. Тогда $\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = \mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) = 2^{j+1}$.

Далее рассмотрим следующие два случая.

Случай 5: $v_2\left(\mathrm{Nm}(p)-1\right) > v_2\left(\mathrm{Nm}(q)-1\right)$.

В этом случае $\mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) = 2^{j+1} \mid \varphi_K(q) = \mathrm{Nm}(q)-1$, значит,

$$\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = 2^{j+1} \mid \left(\mathrm{Nm}(p)-1\right)/2. \tag{22}$$

Получаем, что, с одной стороны, $\left[\frac{\beta}{d}\right] = \left[\frac{\beta}{p}\right] = -1$, а с другой – $b^{(\mathrm{Nm}(p)-1)/2} \equiv 1(\mathrm{mod}\,p)$, что противоречит теореме 1.

Случай 6: $v_2\left(\mathrm{Nm}(p)-1\right) = v_2\left(\mathrm{Nm}(q)-1\right)$.

В данном случае $\left[\frac{\beta}{d}\right] = \left[\frac{\beta}{q}\right]\left[\frac{\beta}{p}\right] = -1$. Без потери общности, будем считать, что $\left[\frac{\beta}{p}\right] = -1$ и $\left[\frac{\beta}{q}\right] = 1$. Согласно теореме 1 получаем, что

$$\beta^{(\mathrm{Nm}(q)-1)/2} \equiv 1(\mathrm{mod}q), \quad \mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = \mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) \mid \left(\mathrm{Nm}(q)-1\right)/2.$$

Так как $v_2\left(\mathrm{Nm}(p)-1\right) = v_2\left(\mathrm{Nm}(q)-1\right)$, то имеем $\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) \mid \left(\mathrm{Nm}(p)-1\right)/2$, а значит, $\beta^{\frac{\mathrm{Nm}(p)-1}{2}} \equiv 1(\mathrm{mod}\,p)$, что противоречит равенству $\left[\frac{\beta}{p}\right] = -1$.

Таким образом, в обоих случаях было получено противоречие, и N является простым элементом.

Замечание 6. По аналогии с [1] с помощью результатов разделов 2, 3 и статьи [18] можно показать, что на основе данного критерия можно предложить полиномиальный алгоритм проверки на простоту идеалов факториальных колец $\mathcal{O}_K$.

Докажем усиленный аналог критерия Эйлера.

Теорема 4. *Предположим, что ERH верна. Пусть* $\mathfrak{n}$ *– нетривиальный идеал нечетной нормы. Тогда* $\mathfrak{n}$ *является простым в* $\mathcal{O}_K$ *тогда и только тогда, когда для любого* $a \in \mathcal{O}_{K,\mathfrak{n}}^{\times}$, $\mathrm{Nm}(a) \leq 12\log^2\left(\Delta_K^2 \mathrm{Nm}(\mathfrak{n})\right)$, *выполнено сравнение*

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\,\mathfrak{n}). \tag{23}$$

Доказательство. Так как $\mathcal{O}_K$ факториально, то $\mathfrak{n}$ – главный идеал, пусть $\mathfrak{n} = (N)$.

Необходимость следует из теоремы 1.

Докажем достаточность. Предположим, что $N \in \mathcal{O}_K \setminus \mathcal{O}_K^{\times}$ не является простым элементом нечетной нормы и для любого $a \in \mathcal{O}_{K,N}^{\times}$, такого что $\mathrm{Nm}(a) \le 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right)$, выполнено

$$a^{(\mathrm{Nm}(N)-1)/2} \equiv \left[\frac{a}{N}\right] (\mathrm{mod}\,N).$$

Введем отображение $\chi : \mathcal{O}_{K,N}^{\times} \to \mathcal{O}_{K,N}^{\times}$, такое что для любого $a \in \mathcal{O}_{K,N}^{\times}$ выполняется

$$\chi(a) = a^{(\mathrm{Nm}(N)-1)/2}\left[\frac{a}{N}\right].$$

Отметим, что χ является эндоморфизмом группы $\mathcal{O}_{K,N}^{\times}$. Из теоремы 1 следует, что χ нетривиален. Применяя утверждение 11, получаем, что существует $\alpha \in \mathcal{O}_{K,N}^{\times}$, такое что

$$\mathrm{Nm}(\alpha) \le 12\log^2\left(\Delta_K^2 \mathrm{Nm}(N)\right), \quad \alpha^{(\mathrm{Nm}(N)-1)/2}\left[\frac{\alpha}{N}\right] \not\equiv 1 (\mathrm{mod}\,N).$$

Получаем противоречие с предположением. Следовательно, N является простым элементом кольца $\mathcal{O}_K$.

Замечание 7. С помощью результатов, плученных в разделах 2, 3 и статьях [16, 18], можно показать, что на основе данного критерия можно предложить полиномиальный алгоритм проверки на простоту идеалов факториальных колец $\mathcal{O}_K$.

Благодарности. Автор выражает благодарность доценту кафедры высшей математики Белорусского государственного университета М. М. Васьковскому за ценные советы и внимание, проявленное к работе.

Acknowledgments. The author is grateful to M. M. Vaskovski, Associate Professor of the Department of Higher Mathematics of Belarusian State University, for valuable advice and attention to the paper.

Список использованных источников

1. Miller, G. Riemann's Hypothesis and Tests for Primality / G. Miller // J. Comput. System Sci. – 1976. – Vol. 13, № 3. – P. 300–317. https://doi.org/10.1016/s0022-0000(76)80043-8

2. Bach, E. Explicit bounds for primality testing and related problems / E. Bach // Math. Comput. – 1990. – Vol. 55, № 191. – P. 355–380. https://doi.org/10.1090/s0025-5718-1990-1023756-8

3. Rabin, M. O. Probabilistic Algorithm for Testing Primality / M. O. Rabin // J. Number Theory. – 1980. – Vol. 12, № 1. – P. 128–138. https://doi.org/10.1016/0022-314X(80)90084-0

4. Solovay, R. A fast Monte-Carlo test for primality / R. Solovay, S. Folker // SIAM J. Comput. – 1977. – Vol. 6, № 1. – P. 84–85. https://doi.org/10.1137/0206006

5. Adleman, M. L. On distinguishing prime numbers from composite numbers / L. M. Adleman, C. Pomerance, R. S. Rumely // Ann. Math. – 1983. – Vol. 117, № 1. – P. 173–206. https://doi.org/10.2307/2006975

6. Agrawal, M. Primes is in P. / M. Agrawal, N. Kayal, N. Saxena // Ann. Math. – 2004. – Vol. 160, № 2. – P. 781–793. https://doi.org/10.4007/annals.2004.160.781

7. Гекке, Э. Лекции по теории алгебраических чисел / Э. Гекке. – М.: Гостехтеоретиздат, 1940. – 260 с.

8. Dekker, T. J. Primes in quadratic fields / T. J. Dekker // CWI Quartetly – 1994. – Vol. 7. – P. 367–394.

9. Vaskouski, M. Primes in quadratic unique factorization domains / M. Vaskouski, N. Kondratyonok, N. Prochorov // J. Number Theory. – 2016. – Vol. 168. – P. 101–116. https://doi.org/10.1016/j.jnt.2016.04.022

10. Howe, E. W. Higher order Carmichael Numbers / E. W. Howe // Math. Comp. – 2000. – Vol. 69, № 232. – P. 1711–1719. https://doi.org/10.1090/s0025-5718-00-01225-4

11. Steel, G. A. Carmichael numbers in number rings / G. A. Steel // J. Number Theory. – 2008. – Vol. 128, № 4. – P. 910–917. https://doi.org/10.1016/j.jnt.2007.08.009

12. Dandan, H. An algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank / H. Dandan, D. Yingpu // Science China Mathematics. – 2017. – Vol. 61, № 5. – P. 783–796. https://doi.org/10.1007/s11425-016-9060-2

13. Cohen, H. A Course in Computational Algebraic Number Theory / H. Cohen. – Springer, 1996. https://doi.org/10.1007/978-3-662-02945-9

14. Post, E. M. Computational Algebraic Number Theory / M. E. Post. – Berlin; Heidelberg: Springer-Verlag, 1993. – 536 p. https://doi.org/10.1007/978-3-0348-8589-8

15. Kannan, R. Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix / R. Kannan, A. Bachem // SIAM J. Comput. – 1979. – Vol. 8, № 4. – P. 499–507. https://doi.org/10.1137/0208040

16. Lenstra, H. W. Computing Jacoby Symbols in Algebraic Number Fiels / H. W. Lenstra // Neieuw Archief voor Wiskunde. – 1995. – P. 421–426.

17. Ankeny, N. C. The Least Quadratic Non Residue / N. C. Ankeny // Ann. Math. – 1952. – Vol. 55, № 1. – P. 65–72. https://doi.org/10.2307/1969420

18. Wikstrom, D. On the l-Ary GCD-Algotihm in Ring of Integers / D. Wikstrom. – Berlin; Heidelberg: Springer-Verlag, 2005. – P. 1189–1201. https://doi.org/10.1007/11523468_96

References

1. Miller G. Riemann's Hypothesis and Tests for Primality. *Journal of Computer and System Sciences*, 1976, vol. 13, no. 3, pp. 300–317. https://doi.org/10.1016/s0022-0000(76)80043-8

2. Bach E. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 1990, vol. 55, no. 191, pp. 355–380. https://doi.org/10.1090/s0025-5718-1990-1023756-8

3. Rabin M. O. Probabilistic Algorithm for Testing Primality. *Journal of Number Theory*, 1980, vol. 12, no. 1, pp. 128–138. https://doi.org/10.1016/0022-314X(80)90084-0

4. Solovay R., Folker S. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 1977, vol. 6, no. 1, pp. 84–85. https://doi.org/10.1137/0206006

5. Adleman M. L., Pomerance C., Rumely R. S. On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, 1983, vol. 117, no. 1, pp. 173–206. https://doi.org/10.2307/2006975

6. Agrawal M., Kayal N., Saxena N. Primes is in P. *Annals of Mathematics*, 2004, vol. 160, no. 2, pp. 781–793. https://doi.org/10.4007/annals.2004.160.781

8. Dekker T. J. Primes in quadratic fields. *CWI Quartetly*, 1994, vol. 7, pp. 367–394.

7. Hecke E. *Lection on theory of algebraic numbers*. Moscow, Gostekhteoretizdat Publ., 1940. 260 p. (in Russian).

9. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory*, 2016, vol. 168, pp. 101–116. https://doi.org/10.1016/j.jnt.2016.04.022

10. Howe E. W. Higher order Carmichael Numbers. *Mathematics of Computation*, 2000, vol. 69, no. 232, pp. 1711–1719. https://doi.org/10.1090/s0025-5718-00-01225-4

11. Steel G. A. Carmichael numbers in number rings. *Journal of Number Theory*, 2008, vol. 128, no. 4, pp. 910–917. https://doi.org/10.1016/j.jnt.2007.08.009

12. Dandan Huang, Deng Yingpu. An algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank. *Science China Mathematics*, 2017, vol. 61, no. 5, pp. 783–796. https://doi.org/10.1007/s11425-016-9060-2

13. Cohen H. A *Course in Computational Algebraic Number Theory.* Springer, 1996. https://doi.org/10.1007/978-3-662-02945-9

14. Post E. M. Computational Algebraic Number Theory. Berlin, Heidelberg, Springer-Verlag, 1993. 536 pp. https://doi.org/10.1007/978-3-0348-8589-8

15. Kannan R., Bachem A. Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix. *SIAM Journal on Computing*, 1979, vol. 8, no. 4, pp. 499–507. https://doi.org/10.1137/0208040

16. Lenstra H. W. Computing Jacoby Symbols in Algebraic Number Fiels. *Neieuw Archief voor Wiskunde*, 1995, pp. 421–426.

17. Ankeny N. C. The Least Quadratic Non Residue. *Annals of Mathematics*, 1952, vol. 55, no. 1. pp. 65–72. https://doi.org/10.2307/1969420

18. Wikstrom D. *On the l-Ary GCD-Algotihm in Ring of Integers*. Berlin, Heidelberg, Springer-Verlag, 2005, pp. 1189–1201. https://doi.org/10.1007/11523468_96

Информация об авторе

Прохоров Николай Петрович – ассистент кафедры высшей математики, Белорусский государственный университет (пр. Независимости, 4, 220072, г. Минск, Республика Беларусь). E-mail: nprohorovminsk@mail.ru

Information about the author

Nikolai P. Prochorov – Assistant of the Department of Higher Mathematics, Belarusian State University (4, Nezavisimosti Ave., 220072, Minsk, Republic of Belarus). E-mail: nprohorovminsk@mail.ru